SIGNPOST

- CROWDOUT

- WHAT HAPPENED?

- GLOBAL SOUTH IMPACT

- POSSIBLE REOCCURENCE?

- INFERRING IMPACT

- POLICY WAKE-UP CALL
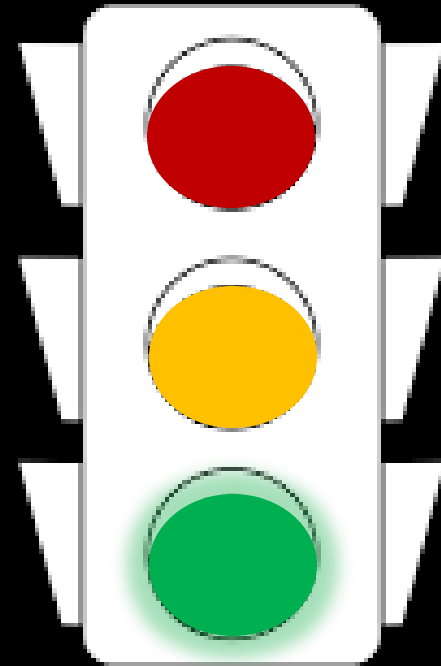
CROWDSTRIKE OUTAGE – A.K.A CROWDOUT

A faulty CrowdStrike update in July 2024 caused global IT outages, affecting 8.5 million devices, disrupting businesses, airports, hospitals, and exposing systems to cybersecurity risks.

BBC

Home News Sport Business Innovation Culture Travel Earth Video Live

Delta Airlines hits out at CrowdStrike, alleging $500m loss

9 August 2024

Share

Nadine Yousif
BBC News

DELTA

JULY 30, 2024

- 4.3 million impacted by HealthEquity data breach
- Microsoft admits CrowdStrike incident far greater than reported
- Proofpoint exploit allows for millions of fake emails

Cyber Securit Headli

Desmond Israel
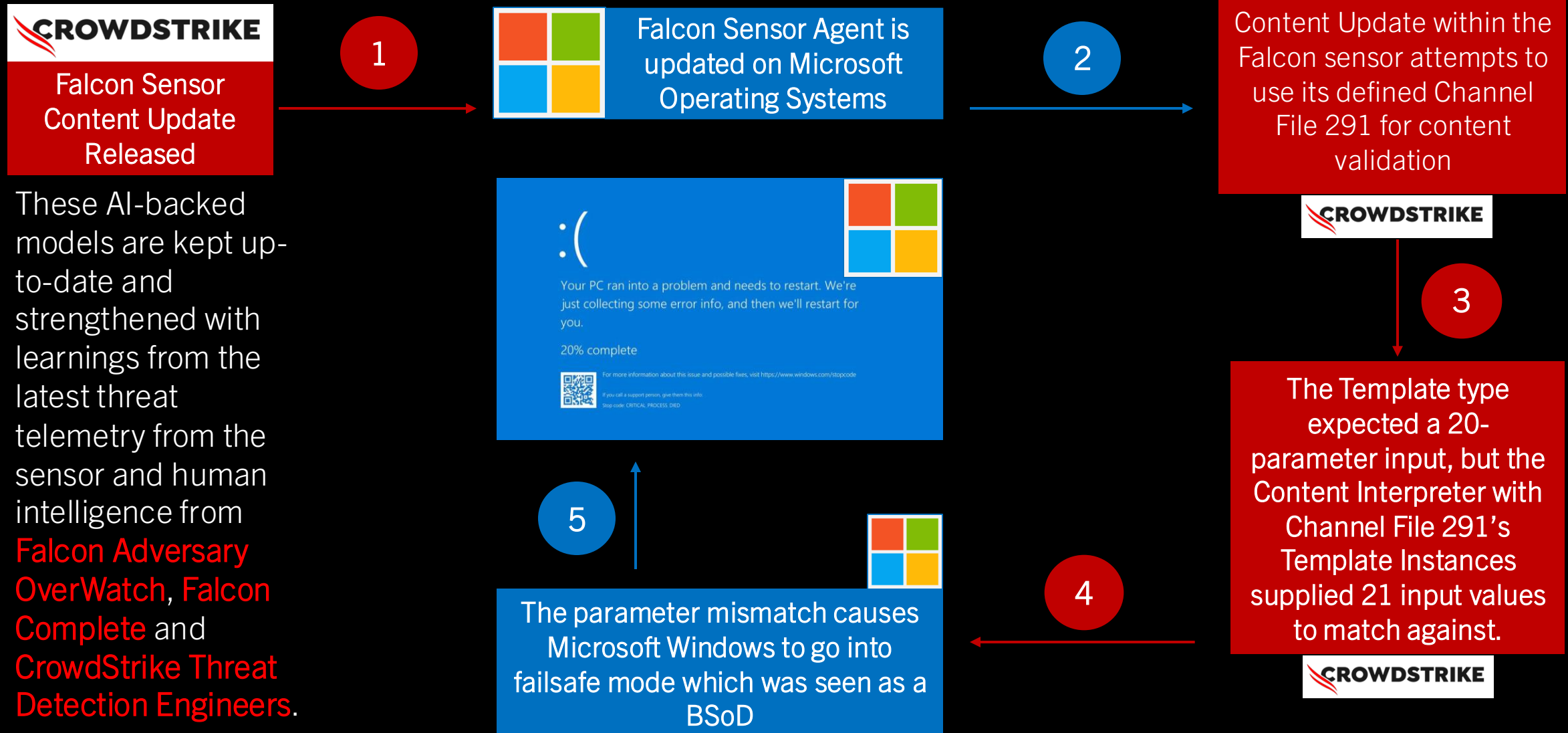Data privacy expert

Technically we call it blue screen of death.

bbcafrica

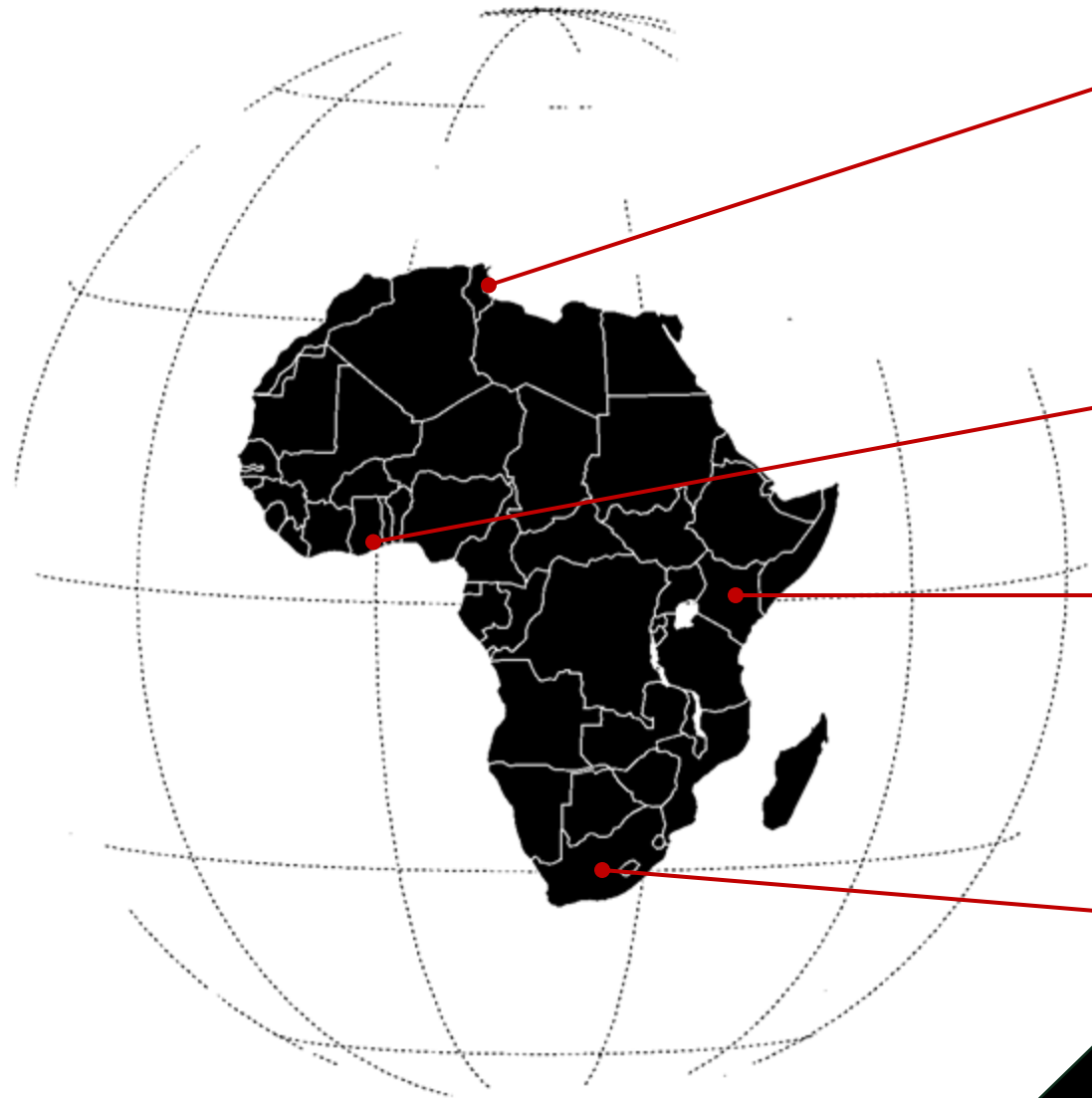A massive tech failure has caused travel ...

1,249
10
96

Israel D. Esq.

CROWDOUT– WHAT HAPPENED?

CROWDSTRIKE

Falcon Sensor Content Update Released

① → Falcon Sensor Agent is updated on Microsoft Operating Systems

② → Content Update within the Falcon sensor attempts to use its defined Channel File 291 for content validation

CROWDSTRIKE

These AI-backed models are kept up-to-date and strengthened with learnings from the latest threat telemetry from the sensor and human intelligence from **Falcon Adversary OverWatch**, **Falcon Complete** and **CrowdStrike Threat Detection Engineers**.

:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:
Stop code: CRITICAL_PROCESS_DIED

③ The Template type expected a 20-parameter input, but the Content Interpreter with Channel File 291's Template Instances supplied 21 input values to match against.

CROWDSTRIKE

⑤ ← The parameter mismatch causes Microsoft Windows to go into failsafe mode which was seen as a BSoD ← ④

Israel D. Esq.

CROWDOUT- GLOBAL SOUTH IMPACT

Tunisia
Aviation - Tunisia experienced temporary airport disruptions. check-in and payment procedures at the electronic levels were temporarily affected, thereby delaying some flights pending the normalization of the systems.

Ghana
Aviation — Airport authorities stated they do not have any impact. **IT Service:** one organisation revealed they had a temproary interruption with their cloud services.

Kenya
Aviation - Airlink booking systems recorded as going down temproarily.

South Africa
Aviation - Airport authorities reported that they do not use Crowdstrike, but airline Airlink reported that its IT network and telephone lines were down.
Banking - 2 major banks (Capitec Bank, and Absa) reported impact on ATMs, and use of bankcards.
Media — eNews Channel Africa could not broadcast

Israel D. Esq.

CROWDOUT- POSSIBLE REOCCURENCE?

2

In 2010, McAfee released a flawed update that mistakenly identified a critical Windows file, "svchost.exe," as a virus. This critical error crashed millions of computers and got them stuck in reboot loops.

4

1

A 2009 Agreement between the European Commission and Microsoft, required they give security software the same level of access to Windows as Microsoft itself

3

In July 2024 a faulty CrowdStrike update caused global IT outages, affecting 8.5 million devices, disrupting businesses, airports, hospitals, and exposing systems to cybersecurity risks.
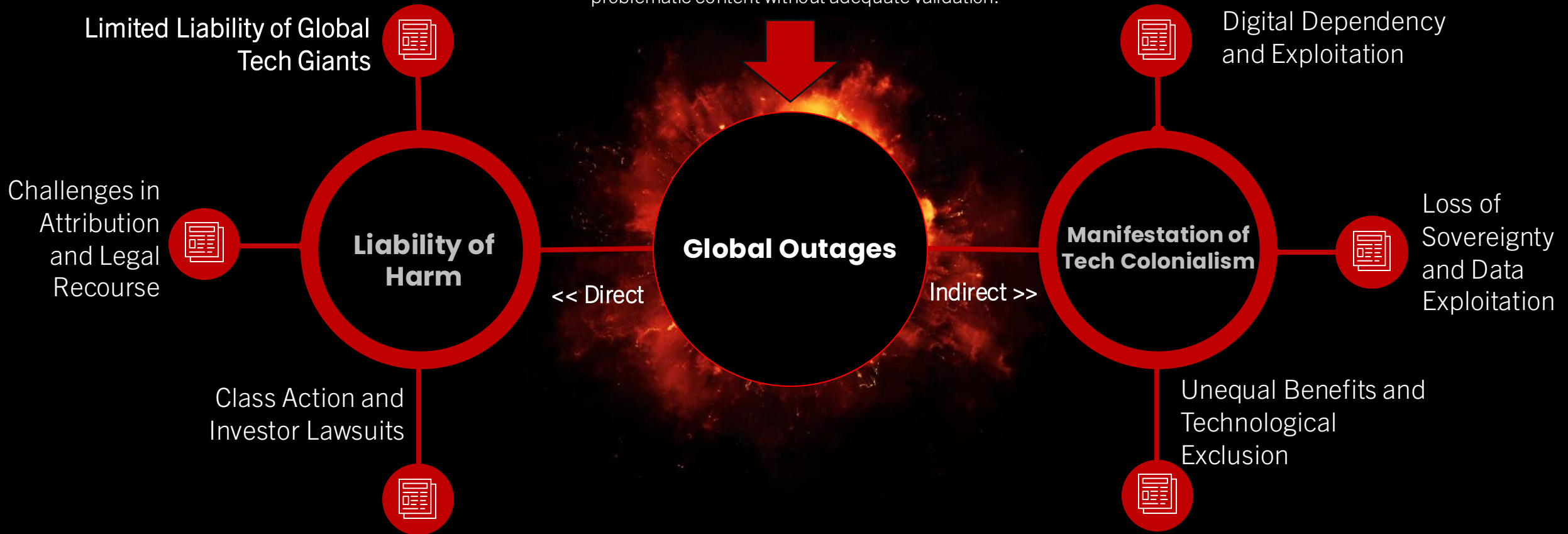
Israel D. Esq.

CROWDOUT- INFERRING THE IMPACT?

Software Development Lifecycle Governance

The lack of a specific test to catch the input mismatch indicates weaknesses in the SDLC processes.

Change Management Failures

The deployment of Channel File 291 containing problematic content without adequate validation.

Limited Liability of Global Tech Giants

Challenges in Attribution and Legal Recourse

Liability of Harm

Class Action and Investor Lawsuits

Global Outages

<< Direct

Indirect >>

Digital Dependency and Exploitation

Manifestation of Tech Colonialism

Loss of Sovereignty and Data Exploitation

Unequal Benefits and Technological Exclusion

CROWDOUT-A POLICY WAKE-UP CALL

1. OVERSIGHT

TECHNOLOGY REGULATORY GAPS

Establish regional technology task forces that collaborate with global governance bodies, ensuring that Africa's needs and risks are incorporated into international standards and best practices for emerging technologies.

2. ACCESS

UNEQUAL ACCESS TO DIGITAL INFRASTRUCTURE

International bodies such as the World Bank and the African Development Bank should collaborate with national governments to invest in building resilient local digital infrastructures. This would mitigate the effects of global outages and promote technological self-sufficiency in the region.

3. COLLABORATION

REGIONAL COLLABORATION ON TECHNOLOGY

The African Union (AU) and other regional bodies must push for collective bargaining power when negotiating with global tech companies. Establishing regional technology policy frameworks and tech standards will empower African nations to mitigate risks from foreign tech dominance.

4. INVESTMENT

INVESTMENT IN LOCAL TECHN-ECOSYSTEMS

Governments and development agencies should invest heavily in local tech talent and infrastructure, promoting African-led innovation. This would reduce reliance on external solutions and help Africa build its own robust digital infrastructure, diminishing the impacts of tech-colonialism and fostering technological self-reliance.

THANK YOU

DESMOND ISRAEL ESQ.

LLM (Natsec/Cybersec) | LLB | BSc (Mgt. with Computing) | BL | Advanced Diploma (IT)

CISSP | CIPM | CCT | CC | Verified Certificate (Cyberwar, Security and Intelligence)

Lawyer and Data Privacy/Information Security Practitioner
Founder & Lead Consultant, Information Security Architects Ltd (*Rapid7 & CodeHunter Partner*)
Adjunct Lecturer, Ghana Institute of Management and Public Administration (GIMPA) School of Law
Consulting Partner, Legal Afrique Unlimited
Technology Policy Researcher / Former Fellow (Center for AI and Digital Policy)
Research Consultant (Child Online Africa)
Memberships: GBA, ISC2, IAPP, IIPGH, ISOC-SIG

desmond.israel@gmail.com

Linkedin.com/in/desmondisrael

@desmond_israel